AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application:

LISTING OF CLAIMS:

1. (withdrawn): A method for preventing bandwidth congestion on a network, said method comprising:

providing at least one origination client connected to an Internet through respective connection points;

providing at least one destination server connected to the Internet;

directing at least one request for connection from at least one of said origination clients to a target destination server over the Internet; and

automatically, upon detecting an overload condition of requests for connection, blocking the origination client, or clients, responsible for said overload condition from accessing the Internet through its, or their, respective connection point(s), but allowing origination client or clients, not responsible for said overload condition to access the Internet.

2. (withdrawn): A method as claimed in claim 1, wherein said connection point through which said origination client(s) is blocked from accessing the Internet, is a connection point which is physically closest to said origination client.

3. (withdrawn): A method as claimed in claim 1, further comprising:

communicating an IP address of said origination client(s) responsible for said overload condition to said connection point(s).

4. (withdrawn): A method as claimed in claim 1, further comprising:

determining whether said blocked origination client should be permitted to gain access to the Internet; and

permitting said blocked origination client access to the Internet if it is determined that said blocked origination client should be permitted access to the Internet.

5. (currently amended): A method for preventing bandwidth congestion on a network, said method comprising:

providing a destination site router connected to a destination site locally and also to an Internet connection;

providing a plurality of origin site routers one or many of which may be connected to an attacking site, wherein each of said plurality of sites has a respective address associated with it;

providing connectivity between said origin and destination routers to the Internet or other wide area networks (WAN), but allowing addresses not corresponding to said attacking site access to the Internet or other WAN;

detecting a bandwidth congestion at said destination site router, wherein said bandwidth congestion originates at said attacking site;

informing said origin site router and other intermediate routers within the Internet, or other WAN, of said bandwidth congestion and of an attacking address corresponding to said

attacking site from which said bandwidth congestion originated, wherein said attacking address is determined from a request packet received from said attacking site;

preventing said attacking address corresponding to said attacking site from being used to gain access to the Internet or other WAN.

6. (original): A method in accordance with claim 5, wherein said informing is performed automatically by said destination router.

7. (original): A method in accordance with claim 5, wherein said informing is performed by human intervention.

8. (original): A method in accordance with claim 5 further comprising:

informing a plurality of remote routers connected to the Internet of said attacking address.

9. (original): A method in accordance with claim 5, wherein said preventing is performed for a predetermined amount of time during which it is determined whether said attacking site is attempting to cause said bandwidth congestion and said attacking site is permitted to gain access to the Internet if it is determined that said attacking site is not attempting to cause said bandwidth congestion.

10. (withdrawn): A network system that prevents bandwidth congestion on a network, said system comprising:

a destination server connected to an Internet through a destination router;

an attack detector operable to detect a denial of service or other Internet-based attack;

an origination client connected to the Internet through an origination router, said origination client being operable to initiate a denial of service or other Internet-based attack,

wherein said attack detector is further operable to communicate an address of said origination client to said origination router to prevent said origination client from being operable to continue said detected denial of service attack, but allowing origination client or clients not initiating the denial of service attack access via said origination router.

11. (withdrawn): A network system according to claim 10, wherein said communication of said identity of said origination client occurs automatically upon detection of said denial of service or other Internet-based attack.

12. (currently amended): A network system that prevents bandwidth congestion on a network, said system comprising:

an origin client router connected to a plurality of clients through an Internet connection, said plurality of clients including an attacking client, and wherein each of said plurality of clients has a respective address associated with it;

a destination site router connected to a destination server, said destination site router or firewall or client further comprising a bandwidth congestion detector operable to detect a bandwidth congestion condition and a communication device operable to communicate said bandwidth congestion condition and said addresses to said plurality of clients;

a router-router connection between said origin client router and said destination site router, wherein said router-router connection provides a discrete amount of access bandwidth by

which said client router and said destination site router can pass data traffic back and forth to each other;

wherein said bandwidth congestion detector detects a bandwidth congestion condition originating at said attacking client and directed to said destination server and automatically informs said origin client router of said attacking client's respective address, and wherein further, said origin client router prevents said address of said attacking client from causing further bandwidth congestion, but allows legitimate client address access to the Internet connection, wherein said attacking client's respective address is determined from a request packet received from said attacking client.

13. (original): A system in accordance with claim 12, wherein said destination site router further informs a plurality of other intermediate routers within the Internet or shared WAN routers in addition to said origin client router.

14. (original): A system in accordance with claim 12, wherein said origin client router prevents said address of said attacking client from gaining access to the router-router connection until such a time when it is determined that said attacking client is no longer attempting to cause bandwidth congestion.

15. (currently amended): A method for preventing bandwidth congestion on a network, said method comprising:

providing a destination site router connected to a destination site locally and also to an Internet connection;

providing a plurality of origin site routers one or many of which may be connected to an attacking site, wherein each of said plurality of sites has a respective address associated with it;

providing connectivity between said origin and destination routers to the Internet or other wide area networks (WAN);

detecting a bandwidth congestion at a firewall connected to said destination site router, wherein said bandwidth congestion originates at said attacking site;

informing said origin site router and other intermediate routers within the Internet, or other WAN, of said bandwidth congestion and of an attacking address corresponding to said attacking site from which said bandwidth congestion originated, wherein said attacking address is determined from a request packet received from said attacking site;

preventing said attacking address corresponding to said attacking site from being used to gain access to the Internet or other WAN, but allowing legitimate addresses access to the Internet or other WAN.

16. (currently amended): A method for preventing bandwidth congestion on a network, said method comprising:

providing a destination site router connected to a destination site locally and also to an Internet connection;

providing a plurality of origin site routers one or many of which may be connected to an attacking site, wherein each of said plurality of sites has a respective address associated with it;

providing connectivity between said origin and destination routers to the Internet or other wide area networks (WAN);

detecting a bandwidth congestion at said destination site, wherein said bandwidth congestion originates at said attacking site;

informing said origin site router and other intermediate routers within the Internet, or other WAN, of said bandwidth congestion and of an attacking address corresponding to said attacking site from which said bandwidth congestion originated, wherein said attacking address is determined from a request packet received from said attacking site;

preventing said attacking address corresponding to said attacking site from being used to gain access to the Internet or other WAN, but allowing legitimate addresses access to the Internet or other WAN.

17. (currently amended): A network system that prevents bandwidth congestion on a network, said system comprising:

an origin client router connected to a plurality of clients through an Internet connection, said plurality of clients including an attacking client, and wherein each of said plurality of clients has a respective address associated with it;

a destination site router connected to a destination server;

a firewall connected to said destination server, said firewall comprising a bandwidth congestion detector operable to detect a bandwidth congestion condition and a communication

device operable to communicate said bandwidth congestion condition and said addresses to said plurality of clients;

a router-router connection between said origin client router and said destination site router, wherein said router-router connection provides a discrete amount of access bandwidth by which said client router and said destination site router can pass data traffic back and forth to each other;

wherein said bandwidth congestion detector detects a bandwidth congestion condition originating at said attacking client and directed to said destination server and automatically informs said origin client router of said attacking client's respective address, and wherein further, said origin client router prevents said address of said attacking client from causing further bandwidth congestion, but allows legitimate clients access to the Internet connection, wherein said attacking client's respective address is determined from a request packet received from said attacking client.

18. (currently amended): A network system that prevents bandwidth congestion on a network, said system comprising:

an origin client router connected to a plurality of clients through an Internet connection, said plurality of clients including an attacking client, and wherein each of said plurality of clients has a respective address associated with it;

a destination site router connected to a destination server, said destination server comprising a bandwidth congestion detector operable to detect a bandwidth congestion condition

and a communication device operable to communicate said bandwidth congestion condition and said addresses to said plurality of clients;

a router-router connection between said origin client router and said destination site router, wherein said router-router connection provides a discrete amount of access bandwidth by which said client router and said destination site router can pass data traffic back and forth to each other;

wherein said bandwidth congestion detector detects a bandwidth congestion condition originating at said attacking client and directed to said destination server and automatically informs said origin client router of said attacking client's respective address, and wherein further, said origin client router prevents said address of said attacking client from causing further bandwidth congestion, but allows legitimate client(s) access to the Internet connection, wherein said attacking client's respective address is determined from a request packet received from said attacking client.

19. (withdrawn): A computer medium storing a program operable to perform the following functions:

detect an internet-based attack directed to a target server from an attacking client;

automatically communicate an address of said attacking client to at least one router through which said attacking client is connected to the Internet so that only said attacking client, but not legitimate client, gain access to the Internet.

20. (withdrawn): A computer medium as claimed in claim 19, further operable to perform the following:

prevent said attacking client from gaining access to the Internet;

determine whether said attacking client is attempting to initiate an Internet-based attack;

permit said attacking client to gain access to the Internet if it is determined that said attacking client is not attempting to initiate an Internet-based attack.

21. (withdrawn): A method as claimed in claim 1, wherein one or more of said destination servers are protected by a respective firewall and wherein said detection of said overload condition is carried out by one of said respective firewalls.

22. (withdrawn): A method as claimed in claim 1, wherein said detection of said overload condition is carried out by said target destination server.

23. (withdrawn): A method as claimed in claim 1, wherein said detection of said overload condition is carried out by a respective target router operably connected to said target destination server.

24. (original): A method in accordance with claim 5, wherein said preventing is performed until a human administrator intervenes after determining whether said attacking site should be permitted to gain access to the Internet.

25. (withdrawn): A network system in accordance with claim 10 wherein said attack detector is located within a firewall device located between said destination server and said origination client.

26. (withdrawn): A network system in accordance with claim 10 wherein said attack detector is located within said destination server.

27. (withdrawn): A network system in accordance with claim 10 wherein said attack detector is located within said destination router.

28. (new): The method in accordance with claim 5, wherein said attacking address corresponding to said attacking site is prevented from being used to gain access to the Internet or other WAN using an access list on said origin site router and other intermediate routers.